JP4115616

Publication Title:

RANDOM CODE GENERATING DEVICE

Abstract:

PURPOSE:To shorten the time required for generating a code by reading in every NS piece of the codes of length (k) generated sequentially from a code converting means, and outputting them after rearranging every NS pieces of the codes in random order by an address generated not from a logical system.

CONSTITUTION:A shift register sequence generator 131 consists of k-pieces of registers and coefficient multipliers and adders less than k-pieces, and generates shift register sequence whose period (n) is longer than NC. The code converting means 123 takes out the required signal sequence from the shift register sequence generator 131, and converts it into the code of the length (k). A code parallel substituting means 133 takes in every NS pieces of the codes of the length (k) generated sequentially from the code converting means 132 in the memory, and rearranges them by every NS pieces in the random order by a means equivalent to the retrieval of a table not by the logical system, and outputs them. But NS is selected so that an integer (m) to satisfy NS <=mXNS <=n exists. Thus, the time required for generating the code can be shortened.

---

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−115616

⑤1Int. Cl.⁵	識別記号	庁内整理番号	㊸公開　平成4年(1992)4月16日
H 03 K 3/84	Z	8221−5J	
H 04 N 7/167		8943−5C	

審査請求　未請求　請求項の数 2　(全19頁)

㊹発明の名称　ランダム符号発生装置

㉑特　願　平2−231481
㉒出　願　平2(1990)8月31日

㉒発明者　沖田　茂　神奈川県横浜市磯子区新杉田町8　株式会社東芝横浜事業所家電技術研究所内
㉑出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
㉔代理人　弁理士 伊藤　進

明　細　書

1．発明の名称

ランダム符号発生装置

2．特許請求の範囲

(1)相異なる長さkの符号をNC個発生するランダム符号発生装置において、

周期nがNCより大なるシフトレジスタ系列を発生するk次のシフトレジスタ系列発生器と、

前記シフトレジスタ系列発生器からの所要の信号系列を取り出し、長さkの符号に変換する符号変換手段と、

前記符号変換手段から逐次的に発生する長さkの符号をNS個ずつメモリーに取込み、理論的体系でなく発生したアドレスをもって、NS個分ずつランダムな順序に並べ換えて出力する符号並換手段と

を備えたことを特徴とするランダム符号発生装置。

ただし、$NC \leq m \times NS \leq n$を満たす整数mが存在するように、NSを選ぶ。

(2)上記並換手段は、検索数NSを並べ換えるごとに変化させることを特徴とするランダム符号発生装置。

3．発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は、パケット伝送、データ通信、データ放送、有料放送等に利用できるランダム符号発生装置に関する。

(従来の技術)

高度なセキュリティが要求されるシステムでは、データパケットを伝送する場合に、データパケットに暗号をかけることが多い。

このようなデータパケットDpは、第16図に示すように、有料放送，データ放送等サービスを識別するためのヘッダHdと、受信者を特定するための個別識別番号Idとが、暗号化領域Dsに付加されており、このような構造のデータパケットDpが伝送路を伝送される。これにより、当該データパケットDpは、伝達先の受信者に確実に受信させるこ

とができる。

第１７図は、上記データ構造を有するデータパケットが伝送される通信システムを示すブロック図である。

第１７図において、個別識別番号Idと、暗号化鍵符号Key とは、次のように使用される。

送信装置100 は、伝送路200 を介して受信装置300(0)～300(Nc－1)にデータパケットDpを送出するようになっている。

上記送信装置100 は、個別識別番号Idと暗号化鍵符号Key とを対応させたテーブル101 を有している。この送信装置100 は、例えば受信装置300(0)にデータパケットを送信する場合、当該テーブル101 から個別識別番号Id(0) と暗号化鍵符号Key(0)を取り出し、暗号化鍵符号Key(0)により暗号化回路102 において送信情報Ifを暗号化し、第２図に示すように、この暗号化したデータを暗号化領域Dsに配置し、かつ暗号化していない個別識別番号Idを付加して伝送路200 に送出する。なお、このテーブル101 に個別識別番号Idに対応させた暗号化鍵符号Key は、ランダム符号発生装置103 から得られる。

受信装置300(0)～300(Nc－1)側では、上述の場合、複号器301(0)は個別識別番号Id(0) が一致するので暗号解読を行うが、その他の複号器301(1)～301(Nc－1)は個別識別番号Id(1) ～Id(Nc －1) が不一致であるので暗号解読ができない。暗号解読には、各受信装置300(0)～300(Nc－1)とも、同一の暗号化鍵符号Key が必要である。この暗号化鍵符号Key は、複号器301(0)～301(Nc－1)の内部メモリ（図示せず）に個別識別番号Id(0) ～Id(Nc －1)とともに書き込まれており、容易には読み出せないようになっている。

ところで、故意に他人の情報を盗用しようとする者に対しては、伝送路200 から個別識別番号Idを比較的容易に取り出すことができても、暗号化鍵符号Key がなければ暗号解読ができないようなシステムとすることにより、他人の情報の盗用を不可能にする安全対策を施している。すなわち、このようなシステムにおいては、個別識別番号Idは暗号解読のアクションの役割しかしておらず、安全対策上は暗号化鍵符号Key が重要な役割を持っていることを意味している。

しかしながら、個別識別番号Idに対する暗号化鍵符号Key の対応づけにおいては、以下の点に留意する必要がある。

（ｉ）個別識別番号Idと暗号化鍵符号Key との関係は、容易に判明する線形結合等で表現され得るものであってはならないこと。

このようにする理由は、個別識別番号Idが伝送路200 上から比較的容易に取り出すことができるので、個別識別番号Idが判明すれば一定の計算により暗号化鍵符号Key がわかってしまうからである。これでは、高度なセキュリティは実現できないことになる。

（ii）個別識別番号Idと暗号化鍵符号Key は一対一の対応とし、同一の暗号化鍵符号Key が異なる個別識別番号Idの組とならないこと。

このようにする理由は、故意に、複号器に入力されるパケットモニタの個別識別番号Idをすげかえることにより、同じ暗号化鍵符号Key をもつ他人の情報を盗用する可能性を防ぐためである。また、偶然にも伝送路200 上で個別識別番号Idの部分がエラーして他人の個別識別番号Idに化け、その化けた個別識別番号Idに対する暗号化鍵符号Key が自分のものとたまたま同一であって、自分の情報が他人に漏れてしまうことがあり得るからである。

さて、上記（ｉ）項については、ランダムな符号系列を用いることによって実現するのが望ましい。例えば個別識別番号Idを順に並べ、逐次的にランダムな符号系列を発生させ、暗号化鍵符号Key として順に対応させてゆく。

また、上記（ii）項の条件を満たすため、過去に発生した符号をメモリに書き込んでおき、発生した符号が過去に発生した符号と重複しないように逐次比較することが必要となる。

第１８図は、上述した暗号化鍵符号Key の発生動作を説明するためのフローチャートであり、このフローチャートはランダム符号発生手段103 で

処理される．

第１８図において、ランダム符号発生手段103が動作し（ステップ2001）、初期設定（ｔ＝０，ｔｃ＝０）がなされる（ステップ2002）．ついで、ランダム符号発生手段103はランダム符号Ｃ(tc)を発生する（ステップ2003）．ついで、定数ｊをリセットし、ｊ＝０とする（ステップ2004）．そして、定数ｊ＝ｔか否かを判定し（ステップ2005）、定数ｊ≠ｔでなければ符号Ｃ(tc)が暗号化鍵符号Key(j)であるか否かを判定し（ステップ2006）、Ｃ(tc)≠Key(j)でなければｊをインクリメント（ｊ＝ｊ＋１）してから（ステップ2007）、再びステップ2005に戻す．

また、定数Ｊ＝ｔか否かを判定し（ステップ2005）、定数ｊ＝ｔであれば符号Ｃ(tc)を暗号化鍵符号Key(j)として出力する（ステップ2008）．ついで、ｔをインクリメント（ｔ＝ｔ＋１）したのち（ステップ2009）、ｔが必要な符号の数Ncかを判定し（ステップ2010）、ｔ≠Ncの場合にtcをインクリメント（tc＝tc＋１）する（ステップ2011）．なお、上記インクリメント（ステップ2011）の場合、ステップ2006でＣ(tc)＝Key(j)のときにも処理される．このインクリメント（ステップ2011）の処理が終了すると、ランダム符号Ｃ(tc)の発生処理に戻る（ステップ2003）．なお、ｔ＝Ncの場合に終了とする（ステップ2012）．

このような処理フローにより、例えば、第６番めの個別識別番号Id(5)に対応する暗号化鍵符号Key(5)については、ランダム符号発生手段103が発生した符号Ｃ(tc)（ここで、tc≧５とする）が、過去に発生した暗号化鍵符号Key(0)～Key(4)のすべて不一致のとき（ステップ2003～2011）、暗号化鍵符号Key(5)＝C(tc)としてメモリに書込み出力する（ステップ2008～2010、2012）．もし、Ｃ(tc)がKey(0)～Key(4)のどれかと一致するならば、次のランダム符号であるＣ(tc＋１)を発生させ、それとKey(0)～Key(4)のそれぞれと比較する．これを全部不一致となるまでくり返す．

このようにして、相異なるランダム符号が順次発生される．

なお、ここでとり上げたランダム符号発生の手段103は、詳しくは、理論的体系をもたない符号を発生する手段のことを意味し、例えば、さいころを振って出た目の数字で符号が決まる符号発生手段のことを指す．以下ランダム符号とはこのような発生手段により発せられた符号とする．

（発明が解決しようとする課題）

ところで、所要の符号の数Ncが非常に大きい場合、問題が発生する．例えば上記個別識別番号Idが３０〔bit〕で構成されている場合、暗号化鍵符号Keyは、$2^{30}\fallingdotseq$１１億個必要となる．このような場合、（１０億＋１）番めの暗号化鍵符号Keyを発生させるためには、過去の１０億個の符号と重複しないように少なくとも１０億回もの比較を行なう必要がある．例えば、１回当たりの比較に要する時間が１０〔μＳ〕であるとすると、１０億回の比較には10^{4}〔Ｓ〕の所要時間がかかり、これは比較するのに２時間半以上時間がかかってしまうという問題がある．

本発明は、上述して問題点に鑑みてなされてものであり、比較の回数を小さくし、かつ符号発生に要する時間を短くすることができるランダム符号発生装置を提供することを目的とする．

〔発明の構成〕

（課題を解決するための手段）

本発明は、上記目的を達成するため、相異なる長さｋの符号をＮＣ個発生するランダム符号発生装置において、周期ｎがＮＣより大なるシフトレジスタ系列を発生するｋ次のシフトレジスタ系列発生器と、前記シフトレジスタ系列発生器からの所要の信号系列を取り出し、長さｋの符号に変換する符号変換手段と、前記符号変換手段から逐次的に発生する長さｋの符号をＮＳ個ずつメモリーに取込み、理論的体系でなく発生したアドレスをもって、ＮＳ個分ずつランダムな順序に並べ換えて出力する符号並換手段とを備えたことを特徴とする．ただし、ＮＣ≦ｍ×ＮＳ≦ｎを満たす整数ｍが存在するように、ＮＳを選ぶ．

また、上記符号並換手段は、検索数ＮＳを並べ換えるごとに変化させればよい．

（作用）

上記従来技術においては、(t＋1)番めのKey(t)の発生にId(t) を対応させた。一般には、Idを連番とすると、Key(t)の引数tとId(t) は同一のものになる。tとId(t) との関係は、ランダムか否かは問題ではない。Key(t)とtと関係がランダムで、tとId(t) もこれとは独立にランダムならばKey(t)とId(t) の関係もランダムである。もちろん、tとId(t) が線形結合の関係にあっても、Key(t)とtがランダムならば、Key(t)とId(t) もランダムである。したがって、本発明では、次の条件を満たす符号を短時間に発生することである。

第①項

発生順tと無関係な符号（ランダム符号Rc(t) ）であること。

第②項

所要の符号数をNcとしたとき、(t－1)≦NcでRc(t) は互いに同一なものが存在しない（重複しない）。

（実施例）

以下、図面に基づいて本発明を説明する。

第１図は本発明の一実施例を示すブロック図である。

第１図において、送信装置１は、伝送路２を介して受信装置３(0) ～３(Nc －1)にデータパケットDpを送出するようになっている。

上記送信装置１は、個別識別番号Idと暗号化鍵符号Key とを対応させたテーブル１１を有している。この送信装置１は、例えば受信装置３(i)（iは任意の整数）にデータパケットを送信する場合、当該テーブル１１から個別識別番号Id(i)と暗号化鍵符号Key(i)を取り出し、暗号化鍵符号Key(i)により暗号化回路１２において送信情報Ifを暗号化し、この暗号化したデータを暗号化領域Dsに配置し、かつ暗号化していない個別識別番号Idを付加して伝送路２に送出する。なお、このテーブル１１に個別識別番号Idに対応させた暗号化鍵符号Key は、ランダム符号発生装置１３から得られる。

ここで、ランダム符号発生装置１３は、相異なる長さkの符号をNC 個発生する装置であって、シフトレジスタ系列発生器１３１と、符号変換手段１３２と、符号並換手段１３３とで次のように構成されている。

上記シフトレジスタ系列発生器１３１は、k個のレジスタ、１個以上k個以下の係数器、１個以上k個以下の加算器からなり、周期nがNC より大なるシフトレジスタ系列を発生する。

上記符号変換手段１３２は、前記シフトレジスタ系列発生器１３１のシフトレジスタの出力、係数器の出力、あるいは加算器の出力から所要の信号系列を取り出して長さkの符号に変換する。

上記符号並換手段１３３は、前記符号変換手段１３２から逐次的に発生する長さkの符号をNS 個ずつメモリーに取込み、理論的体系によらないテーブルの検索に準ずる手段によりNS 個分ずつランダムな順序に並べ換えて出力する。

ただし、NC ≦m×NS ≦nを満たす整数mが存在するように、NS は選ばれている。

ランダム符号発生装置１３は、上述したように構成されている。

第２図は、シフトレジスタ系列発生器１３１の一例であって、線形帰還シフトレジスタ回路で構成した例を示すブロック図である。

この線形帰還シフトレジスタ回路で構成したシフトレジスタ系列発生器１３１は、クロック入力端子CTを設けたk個のレジスタRE10～RE1k-1を直列接続してなるレジスタと、係数（－h0～－hk-1 ）のk個の係数器K10～K1k-1と、（k＋1）個の加算器AD11～AD1kと、スイッチSWとからなり、加算器AD1kに入力端子TIを接続し、レジスタRE11の出力に出力端子T0を接続している。

各レジスタRE10～RE1k-1の各出力はat+k-1～atで示され、係数器K1iの出力は（－hi・at+i ）で示され、加算器AD1iの出力は（－hi・at+i ）を0～iまで加算した値を示している。

このようなシフトレジスタ系列発生器１０１において、まず、スイッチSWを最初に初期値を入

力端子ＴＩより入力するときに開いておき、クロック入端子ＣＴよりクロックをｋ個入力すると、各レジスタＲＥ10～ＲＥ1k-1に初期値がセットされる。その後、入力端子ＴＩの入力信号を“０”とし、スイッチＳＷを閉じてクロック入端子ＣＴからクロック信号を入力する。これにより、各レジスタＲＥ10～ＲＥ1k-1の内容を次々に移すことをくり返すと、出力端子Ｔ０からシフトレジスタ系列が出力される。そして、（ｎ－１）クロック目に各レジスタＲＥ10～ＲＥ１k-1の内容が元の初期値に戻る。このとき、このｋ次のシフトレジスタ系列は周期ｎをもつという。

第３図は、シフトレジスタ系列発生器１３１の他の例であって、線形シフトレジスタ回路で構成した例を示すブロック図である。

この線形シフトレジスタ回路で構成したシフトレジスタ系列発生器１３１は、クロック入力端子ＣＴを設けたｋ個のレジスタＲＥ21～ＲＥ2kを直列接続してなるレジスタと、係数（－ｈ０～－ｈｋ-１）のｋ個の係数器Ｋ20～Ｋ2k-1と、ｋ個の加算器ＡＤ20～ＡＤ[illegible]と、スイッチＳＷとからなり、加算器ＡＤ20に入力端子ＴＩを接続し、レジスタＲＥ2kの出力に出力端子Ｔ０を接続している。なお、スイッチＳＷは、最初初期値を入力端子ＴＩより入力するときに開いておく。

このような線形シフトレジスタ回路で構成したシフトレジスタ系列発生器１３１によっても第２図と同様にｋ次のシフトレジスタ系列を得ることができる。

ところで、上記各シフトレジスタ系列発生器１３１において、扱う符号が２元シンボル｛“０”、“１”｝で構成されるならば、これらは２を法とする乗算、加算になる。また、ｑ元シンボル｛０，１，…，ｑ－１｝ならば、ｑを法とする乗算、加算になる。したがって、例えばｑ＝３の場合には、ｋ＝３次のシフトレジスタ系列が発生することになる。

第４図は、ｑ＝３の場合のシフトレジスタ系列発生器１３１の実構成例であって、３元Ｍ系列符号発生回路を示している。

この３元Ｍ系列符号のシフトレジスタ系列発生器１３１ａは、３個のレジスタＲＥ30～ＲＥ32を直列接続してなるレジスタと、係数（－ｈ０またはｈ１）の１個の係数器Ｋ30と、２個の加算器ＡＤ31～ＡＤ32と、スイッチＳＷとからなり、加算器ＡＤ32に入力端子ＴＩを接続している。各レジスタＲＥ30～ＲＥ32の出力をＱ〔０〕～Ｑ〔２〕とする。

この実施例は、シフトレジスタ系列の中でも同一の段数で周期が最大の系列（Ｍ系列）を発生する。一般にＭ系列の周期は、ｎ＝ｑ^{k}－１である。このような周期ｎをもつｋ次のシフトレジスタ系列発生器からは、適当に符号を取り出すことにより長さｋの符号が周期ｎで得られる。例えば、第４図の実例のように、ｑ＝３の場合のｋ＝３次のシフトレジスタ系列発生器１３１ａからは、ｎ＝（３^{3}－１）＝（２７－１）＝２６が得られ、一周期が２６をもつシフトレジスタ系列が発生することになる。

ここで、係数器Ｋ30は、｛－ｈ０＝（－１ mod ３）＝２｝、または｛－ｈ１＝（－２ mod ３）＝１｝となる。また、mod ３は、３を法とする演算を意味し、上記シフトレジスタ系列発生器１３１ａは生成多項式Ｈ(x)＝ｘ^{3}＋２ｘ＋１を満足する。

このようなシフトレジスタ系列発生器１３１ａにより得られたシフトレジスタ系列を第５図に示す。

第５図（ａ）は、レジスタＲＥ30～ＲＥ32に初期値（“０”“１”“０”）をセットしたときに、シフトレジスタ系列発生器１３１ａから得られるシフトレジスタ系列の説明図である。

時間(time)の経過に伴う、各レジスタＲＥ30～ＲＥ32の出力Ｑ[2]，Ｑ[1]，Ｑ[0] の値と、十進法(ma)の値とが示されている。

ここで、各レジスタＲＥ30～ＲＥ32の出力Ｑ[2]，Ｑ[1]，Ｑ[0] の値を十進法(ma)に変換するためには、

ma＝３^{2}×Ｑ[2] ＋３×Ｑ[1] ＋Ｑ[0]

を使用すればよい。

第５図（ｂ）は、レジスタＲＥ30～ＲＥ32に初期値（"２" "０" "０"）をセットした場合に、シフトレジスタ系列発生器１３１ａから得られるシフトレジスタ系列の説明図である。

このような初期値の場合の時間(time)の経過に対する、各レジスタＲＥ30～ＲＥ32の出力Ｑ[2]，Ｑ[1]，Ｑ[0] の値と、十進法(ma)の値とが示されている。

この符号系列の特徴は、シフトレジスタ系列の状態が、各レジスタＲＥ30～ＲＥ32の内部状態の組合せで一意に決まる点である。したがって、この例では、第５図（ａ）または同図（ｂ）に示すように、初期値のいかんによらず、

（Ｑ[2]，Ｑ[1]，Ｑ[0] ）＝（２００）の次のタイムスロットでは、必ず（Ｑ[2]，Ｑ[1]，Ｑ[0] ）＝（０２０）となる。

次に、符号変換手段１３２の構成例を説明することにする。

符号変換手段１３２の一番簡単な構成は、シフトレジスタ系列発生器１３１の具体例として第４図に示した回路における各レジスタＲＥ30～ＲＥ32の出力をそのまま取り出すようにした回路構成とすればよい。

このような符号変換手段１３２によれば、逐次的（シーケンシャル）に出力される符号系列の連続したｎ個は互いに重複することがない（同一のものはない）。

これらの符号系列は、ｎ≧Ｎｃとすることにより、上記条件②項を満足することになる。また、この条件②項を満足するために、従来必要だった過去に発生した符号との比較は、本実施例では不要となる。しかしながら、この構成例は、上記の条件①項を満たしてはいない。なぜなら、これらの符号系列は、線形演算により発生されたものだからである。

そこで、上記条件①項を満たすためには、上記符号変換手段１３２の出力Ｌ(t) に対して、符号並換手段１３３を用いて符号の並べ換えをすればよい。

まず、符号並換手段１３３は、上記符号変換手段１３２の出力Ｌ(t) より逐次的に得られるＮｓ個の符号の組Ｌ(t)，Ｌ(t＋１)，…，Ｌ(t＋Ｎｓ－1)をメモリに、順に書き込む。次に、符号並換手段１３３は、理論的体系を持たないメモリアドレスを発生させる手段により、前記データを前記メモリから取り出してランダムに並べ換える。この出力を、Ｒ(t)，Ｒ(t＋１)，…，Ｒ(t＋Ｎｓ)とする。このとき、並べ換えるのは、Ｎｓ個の符号の範囲内である。したがって、過去に発生した符号と重複しないように比較する符号の対象は、(t＋Ｎｓ－1)番めの符号発生のとき最大であって、（Ｎｓ－1)個である。すなわち、１億番目の符号発生においても、１０億番目の符号発生においても、比較する符号の対象は（Ｎｓ－1)個以下となる。

第６図は、上記構成の動作を説明をするために示すフローチャートである。

まず、送信装置１において動作が開始する（ステップ601 ）。ついで、送信装置１がリセットされ、ランダム符号発生装置１３もリセット（ｔ＝０，ｔｃ＝０）されることになる（ステップ601 ）。ついで、ランダム符号発生装置１３のシフトレジスタ系列発生器１３１は、シフトレジスタ系列を発生する（ステップ602 ）。ついで、例えば第４図のシフトレジスタ系列発生器１３１ａの各レジスタの出力から直接取り出すことにより構成された符号変換手段１３２をもって、長さｋの符号への変換を行い、出力Ｌ(t)，Ｌ(t＋１)，…，Ｌ(t＋Ｎｓ－1)を得る（ステップ６04）。

ついで、符号並換手段１３３は、上記符号変換手段１３２の出力Ｌ(t) より逐次的に得られるＮｓ個の符号の組Ｌ(t)，Ｌ(t＋１)，…，Ｌ(t＋Ｎｓ－1)をメモリに、順に書き込む（ステップ605)。これは、以下のようにする。

符号並換手段１３３のメモリの
０番地のアドレスにＬ(t) を、
１番地のアドレスにＬ(t＋１)を、
……，
ｉ番地のアドレスにＬ(t＋ｉ)を、
……，

（Ｎｓ－1)番地のアドレスにＬ(t+Ｎｓ－1)をそれぞれ書き込む。

次に、ｉ＝０とする（ステップ606 ）。そして、理論的体系を持たないメモリアドレスを発生させる手段により、ランダムアドレスＣ(t) を発生させる（ステップ607 ）。ただし、ランダムアドレスＣ(t) は、０≦Ｃ(t) ≦（Ｎｓ－1)の関係が成立するものとする。

ついで、定数ｊをリセットし、ｊ＝０とする（ステップ608 ）。そして、定数ｊ＝ｉか否かを判定し（ステップ609 ）、定数ｊ＝ｉでなければＬ(t+Ｃ(t))＝Ｒ(t+ｊ)であるか否かを判定し（ステップ610 ）、Ｌ(t+Ｃ(t))＝Ｒ(t+ｊ)でなければｊをインクリメント（ｊ＝ｊ＋１）してから（ステップ611 ）、再び定数ｊ＝ｉか否かの判定（ステップ609 ）に戻す。

また、定数ｊ＝ｔか否かを判定し（ステップ609 ）、定数ｊ＝ｔであればＲ(t+ｊ)をＬ(t+Ｃ(t))として出力する（ステップ612 ）。ついで、ｉをインクリメント（ｉ＝ｉ＋１）したのち（ステップ613 ）、ｉが[illegible]な符号の数Ｎｃかを判定し（ステップ614 ）、ｉ≠Ｎｃの場合にｔｃをインクリメント（ｔｃ＝ｔｃ＋１）する（ステップ615 ）。なお、上記ｔｃのインクリメント（ステップ615 ）の処理は、Ｌ(t+Ｃ(t))＝Ｒ(t+ｊ)と判定されたときにも（ステップ610 ）、実行される。このインクリメント（ステップ615 ）の処理が終了すると、ランダムアドレスＣ(tc)の発生処理に戻る（ステップ607 ）。

なお、ｉ＝Ｎｃの場合（ステップ614 ）、ｔ＝ｔ＋Ｎｓの処理をし（ステップ616 ）、ついで、〔ｔ≦Ｎｃ－１〕であるなら（ステップ617 ）、シストレジスタ系列の発生処理（ステップ602 ）に戻る。また、〔ｔ＞Ｎｃ－１〕であるなら（ステップ617 ）、全ての処理を終了する（ステップ618 ）。

このように動作することにより、シフトレジスタ系列発生器１３１からシフトレジスタ系列が発生し、このシフトレジスタ系列を符号変換手段１３２で符号変換し、その符号変換した出力を符号並換手段１３３でランダムに並べ換えることにより、ランダム符号が発生することになる。

このように本実施例で発生するランダム符号は、従来のものと比べて短時間で得ることができることになる。これを以下に説明する。

従来の方法では、第１８図のフローチャートに示すようにｔ番めの出力は、比較の対象が（ｔ－１）個存在した。これと同様なフローでＮｓ個の符号をランダムな順序に出力するとすれば、Ｒ(t+ｉ)，〔ただし、０≦ｉ≦（Ｎｓ－1)である〕の発生においては、（ｉ－１）個が比較の対象となる。第６図に示すフローチャートにおいて、ステップ605 以降のステップが符号並換手段１３３で処理される。

上記メモリアドレスＣ(t) の発生確率を一様（それぞれ１／Ｎｓ）とすると、Ｒ(t+Ｎｓ－1)を発生するのに必要なメモリの読み出し回数は、平均Ｎｓ回である。このうち、（Ｎｓ－1)回は、（Ｎｓ－2)個の符号Ｒ(t)，Ｒ(t+１)，…，Ｒ(t+Ｎｓ－2)のいずれかと一致する。このとき読み出した符号について、この順に比較するとすれば、それぞれと一致する確率は等しく、１／Ｎｓである。また、一致検出までの比較（第６図のステップ607 ～609 による）の回数は、それぞれ、１，２，…，（Ｎｓ－１）であるから、この場合の平均比較回数は

｛１／（Ｎｓ－1)｝×｛１＋２＋（Ｎｓ－1)｝
＝Ｎｓ／Ｎｓ－１　　…（１）

である。

最後のＮｓ回目は、必ず（Ｎｓ－1)回の比較を行うので、Ｒ(t+Ｎｓ－1)を発生するのに比較する平均回数Ｎcmpは、

Ｎcmp＝（Ｎｓ－1)×｛Ｎｓ／（Ｎｓ－1)｝
＋（Ｎｓ－1)＝２Ｎｓ－１　…（２）

である。

Ｒ(t+ｉ)，ただし、０≦ｉ＜（Ｎｓ－1)　を発生するときの比較対象は、（ｉ－１）個の符号なので、平均比較回数は、上記（２）式のＮcmpより小である。

例えば、Ｎｓ≒100としたとき、上記（２）式

より平均比較回数は、せいぜい199 程度であり、従来では（１０億＋１）番目の符号出力に対して、１０億回以上の比較を必要としていた方法に比べ格段に発生時間を短縮できる。

上述の実施例の場合を従来のものと比較してみると、199 ／10^9 ≒ $2/10^7$ 以下に短縮することができることを意味している。

なお、Ｎｓを毎回固定とすると、シフトレジスタ系列の周期ｎに関して、

$$Nc \leqq m \times Ns \leqq n \qquad \cdots (3)$$

なる整数ｍが存在するという条件が必要である（実施例参照）。

また、並べかえの個数Ｎｓを可変とすることも可能であり、このとき i 番めの並べ換えをＮｓｉとすると、上記第（３）式は、

$$Nc \leqq \sum_{i=1}^{m} Nsi \leqq n \qquad \cdots (4)$$

という整数ｍが存在するという条件におき変わることになる。

一般に、Ｎｃとｎが近い数のとき、最後のｍ番めの並べ換えにて、第（４）式を満たすように、Ｎｓを小さく選べばよい。例えば、Ｎｃ＝250 であって、ｎ＝255 のとき、

Ｎｓ１＝Ｎｓ２＝Ｎｓ３＝80であるとすると、

$$250 - 80 \times 3 \leqq Nsm = Ns4 \leqq 255 - 80 \times 3$$

$$10 \leqq Ns4 \leqq 15 \qquad \cdots (5)$$

とすれば、上記第（４）式は満たされることになる。

また、Ｎｓを毎回ランダムに変化させると、Ｒ(t) のランダム性も大となる。

なお、長さｋの符号への符号変換手段１３２は、ハードウェアイメージで、Ｎ個の符号並換手段１３３はソフトウェアイメージで説明してきたが、相方ともソフトでもハードでも実現できる。例えば、ｋ次ソフトレジスタ系列の発生は、レジスタの内容をまねるようにプログラムを組めば発生できる。

本発明の一実施例は、上記したようになっている。

次に、本発明の他の実施例を以下に説明する。

第７図は、長さｋ＝８のシフトレジスタ系列発生器の構成例を示すブロック図である。

第７図に示す８次のシフトレジスタ系列発生回路811 は、第２図に示す線形帰還シフトレジスタ回路の変形例である。

この図では、レジスタ800 ～807 と、加算器808 ～810 とで、８次のシフトレジスタ系列発生回路811 が構成されている。このシフトレジスタ系列発生回路811 は、第２図の構成とは異なって初期値を入力するための入力端子ＴＩと、スイッチＳＷと、シフトさせるためのクロック入力端子ＣＴとを省略している。このシフトレジスタ系列発生回路811 の信号のうち、Ｑ[7]，Ｑ[6]，Ｑ[5]，Ｑ[4]，Ｑ[3]，Ｑ[2]，Ｑ[1]，Ｑ[0] を選ぶことにより、長さｋの符号を得られる。

このとき、長さ８の符号への符号変換手段812 は有形無形であるが、一般には第８図に示される論理回路で構成できる。

第８図において、論理回路812aは、Ｑ[7]，Ｑ[6]，Ｑ[5]，Ｑ[4]，Ｑ[3]，Ｑ[2]，Ｑ[1]，Ｑ０，Ｑ′[4]，Ｑ′[3]，Ｑ′[2] の入力端子と、Ｌ(t) ＝（ｂ７，ｂ６，ｂ５，ｂ４，ｂ３，ｂ２，ｂ１，ｂ０）の出力端子と、およびセレクト信号入力端子とを設けている。

ただし、信号の組合せ方にはある制限がある。前にも説明したように、シフトレジスタ系列発生器の状態は、シフトレジスタ811 の内容で一意に決定される。発生された符号Ｌ(t) が、周期ｎをもつためには、Ｌ(t) と各レジスタの内容の組合せが一対一対応とならなければならない。したがって、Ｑ[4] と、Ｑ′[4] とを同時に選ぶと、レジスタ804 の内容が重複するので、他のレジスタのうちどれかひとつは抜けることとなる。

一般には、第２図で示す型式のシフトレジスタ発生回路を用いた場合、右からｉ番めのレジスタに関しては、a_{t+i}、$-h_i \cdot a_{t+i}$、$\Sigma(-h_i \cdot a_{t+i})$ のうち少なくともどれかひとつを符号Ｌ(t) の要点として選ぶことが、Ｌ(t) が周期ｎをもつことの必要十分条件である。また、当然のことながら、第８図においてＬ(t) の発生途中でセレクト信号を変化させ、組合せを変えると周

期ｎは保証されない。

第７図のシフトレジスタ系列発生回路811を用いた生成多項式Ｈ(x)は、

$H(x) = x^8 + x^4 + x^3 + x^2 + 1$

の場合の長さ８の符号Ｌ(t)の発生例を次に説明することにする。

第９図(1)～同図(3)は、初期値を（Ｑ[7],Ｑ[6],Ｑ[5],Ｑ[4],Ｑ[3],Ｑ[2],Ｑ[1],Ｑ[0]）＝（１０１０１０１１）とすると、時刻(time)に対する、出力Ｑ[7],Ｑ[6],Ｑ[5],Ｑ[4],Ｑ[3],Ｑ[2],Ｑ[1],Ｑ[0]の値と、出力Ｑ´[4],Ｑ´[3],Ｑ´[2]の値と、十六進数ｍａ,ｍｂ,ｍｃの値を示している。

また、十六進数ｍａ,ｍｂ,ｍｃは、長さ８への変換の例として、

ｍａ＝（Ｑ[7],Ｑ[6],Ｑ[5],Ｑ[4],Ｑ[3],Ｑ[2],Ｑ[1],Ｑ[0]）

ｍｂ＝（Ｑ[7],Ｑ[6],Ｑ[5],Ｑ´[4],Ｑ´[3],Ｑ´[2],Ｑ[1],Ｑ[0]）

ｍｃ＝（Ｑ[7],Ｑ[6],Ｑ[5],Ｑ´[4],Ｑ´[3],Ｑ´[2],Ｑ[1],Ｑ[0]）

で求められる。

第１０図は長さ８の符号への符号変換手段を、シリアル／パラレル変換回路を用いて構成した例を示すブロック図である。

長さ８の符号への符号変換手段812bは、レジスタＲＥ80～ＲＥ87を直列接続し、各レジスタＲＥ80～ＲＥ87にクロックを入力可能し、レジスタＲＥ88に出力Ｑ[0]を入力し、かつ各レジスタＲＥ80～ＲＥ88の出力から出力Ｌ(t)＝（ｂ７，ｂ６，ｂ５，ｂ４，ｂ３，ｂ２，ｂ１，ｂ０）を得るようしたものである。

これのクロック信号は、第７図に示すシフトレジスタ系列発生回路811のシフトクロックと同一のものである。この場合、Ｌ(t)は８クロック前の第７図のシフトレジスタ系列発生回路811の各レジスタの内容と一致する。

シフトレジスタ系列は、Ｍ系列だけとは限らない。

第１１図に、Ｍ系列でない８次のシフトレジスタ系列発生器の実施例を示す。

Ｍ系列でない８次のシフトレジスタ系列発生器811bは、第７図のシフトレジスタ系列発生器811とは、加算器808a,809a,810a,810bで、出力Ｑ[7],Ｑ[6],Ｑ[4],Ｑ[1]を加算して、レジスタ807に入力し、Ｑ´[7],Ｑ´[6],Ｑ´[4],Ｑ´[1]を得られるようにした点が異なる。

このシフトレジスタ系列発生器811bによれば、生成多項式Ｈ(x)は、

$H(x) = (x+1)^3 (x^5 + x^2 + 1)$

$= x^8 + x^7 + x^6 + x^4 + x + 1$

として得られる。

これは、初期値をＱ[7]～Ｑ[0]の順に、（１０００００００）のようにセットすると、

$n = 4 \times 31 = 124$ …（６）

の周期をもつ系列を発生する。

この系列を、長さ８の符号の符号変換手段により以下のように変換する。

第１２図（１）、同図（２）は、初期値が（Ｑ[7]～Ｑ[0]）＝（１０００００００）のときに、一周期ｎ＝124における時刻（time）に対する、出力Ｑ[7]～Ｑ[0]の値と、出力Ｑ´[7],Ｑ´[6],Ｑ´[4],Ｑ´[1]の値と、三つの十六進数ｍａ,ｍｂ,ｍｃの値（符号変換手段の値）をそれぞれ示されている。

また、十六進数ｍａ,ｍｂ,ｍｃは、長さ８への変換の例として、

ｍａ＝（Ｑ[7],Ｑ[6],Ｑ[5],Ｑ[4],Ｑ[3],Ｑ[2],Ｑ[1],Ｑ[0]）

ｍｂ＝（Ｑ´[7],Ｑ´[6],Ｑ[5],Ｑ´[4],Ｑ[3],Ｑ[2],Ｑ´[1],Ｑ[0]）

ｍｃ＝（Ｑ´[7],Ｑ[6],Ｑ[5],Ｑ´[4],Ｑ[3],Ｑ[2],Ｑ´[1],Ｑ[0]）

で求められる。

第１３図は、初期値が（Ｑ[7]～Ｑ[0]）＝（１１０１０００００）のときに、一周期ｎ＝64における時刻（time）に対する、出力Ｑ[7]～Ｑ[0]の値と、出力Ｑ´[7],Ｑ´[6],Ｑ´[4],Ｑ´[1]の値と、三つの十六進数ｍａ,ｍｂ,ｍｃの値（符号変換手段の値）をそれぞれ示されている。

また、十六進数ma,mb,mcは、長さ8への変換の例として、

ma = (Q[7],Q[6],Q[5],Q[4],Q[3],Q[2],Q[1],Q[0])

mb = (Q′[7],Q′[6],Q[5],Q′[4],Q[3],Q[2],Q′[1],Q[0])

mc = (Q′[7],Q[6],Q[5],Q′[4],Q[3],Q[2],Q′[1],Q[0])

で求められる。

上記は、同じ回路で初期値のみを違えたものである。簡便には、第15図と16図で取り得ないレジスタの値を初期値として与えてみると、n=124の場合と、n=62の場合とで、Sa同士で比較すると、一致する符号がないことがわかる。これは、シフトレジスタ系列発生器の状態がレジスタの内容に代表されるからで、124種のAグループと、62種のBグループとが存在し、それぞれグループ内のどの初期値を読み込んでも周期n=124か、n=62の符号L(t)を発生することができる。また、初期値の操作により、L(t)としてAグループとBグループに対応する符号が混在するものも得ることができる。例えば、初期値(10000000)より順次符号L(t)を発生させ、途中で時間(time)(t=50)において、強制的に(11010000)を読み込ませるとAグループからBグループに移る。

そして、L(50)からL(50+61)を発生したとこれで、再び初期値を、第12図(1)の時間(time)(t=50)に対応するところの(10010011)を読み込ませると、再びAグループにもどる。このように、n=124+62=186個の重複しない符号L(t)を得ることができるわけである。

シフトレジスタ系列の特徴は、こうしたことが第12図、第13図をあらかじめ持っていなくても逐次的な操作で可能であることが大きな特徴であり、nが大の場合に有効である。

次に、Nsの符号の符号並換手段の実施例を第14図に示す。

並べ換えの動作は、第6図に示すフローチャートにより行うものとし、Ns=30の場合の例である。

L(t)の符号は並べ換え前で、第9図(1)のmaと同一である。R(t)は、並べ換え後で最初の90個を示す。Ns個内での比較は、符号自体で行ったが、過去に発生したメモリアドレスとの比較でも可能である。L(t)のNs個をランダムに並べ換えることは、0～(Ns-1)のアドレスをランダムに、しかも重複しないで発生することに等価である。

したがって、たとえばアドレスを〔7,0,11,10〕と過去に発生したならば、次に発生するアドレスは〔7,0,11,10〕以外であればよい。

このために、第6図のフローチャートにおいて、ステップ610での比較は、アドレスであるもの同士を比較すればよい(つまり、C(t)=iかとする)。この場合、Ns=30ならば、jは0≦j≦29なので、5ビットで表現でき、その比較は5ビットでよいことになる。もしも、R(t)として、50ビット必要ならば、比較のビット数は、1/10になる。

また、メモリアドレスの発生順序を、Ns個の並べ換えごとに変えることは必ずしも必要でなく、テーブルとして固定のランダムなアドレスのセットを持っていてもよい。この場合は、第6図のフローチャートのステップ601は、「t←0、tc←0」について、「t←0」とし、同図フローチャートのステップ608の「j←0」を「j←0、tc←0」とすることに相当する。

第15図は、第14図のL(t)、R(t)のものと同じ系列であり、Nc≦m×Ns≦n(…(3)式)を満たさないものの例である。

すなわち、上記例は、上記第(3)式を満たさないときは、この例のように、R(242)=(29)hex=(00101001)=R(10)

において重複することになる。

このような実施例によっても、符号並換手段が実現することができる。

本発明の実施例は、上述したように、必要なランダム符号R(t)の数Ncが大きいとき、符号発

生に要する時間の短縮できる効果がある。また、本実施例では、R(t)の符号発生時に要する時間の比率は、並べ換えの個数Nsに対し、{(2Ns−1)／t}以下であり、t＝10⁹、Ns＝100とすれば、2／10⁷以下の時間で発生できることになる。

〔発明の効果〕

以上説明してきたとおり、本発明は、必要なランダム符号R(t)の数Ncが大きいとき、符号発生に要する時間の短縮できる効果がある。また、本発明は、R(t)の符号発生時に要する時間の比率は並べ換えの個数に対して著しく短い時間で発生することができる。

4．図面の簡単な説明

第1図は本発明の一実施例の全体構成を示すブロック図、第2図は同実施例の線形帰還形のシフトレジスタ系列発生器を示すブロック図、第3図は同実施例の線形形のシフトレジスタ系列発生器を示すブロック図、第4図は同実施例の3元M系列のシフトレジスタ系列発生器の具体例を示すブロック図、第5図は第4図の発生器で得られる符号の発生例を示す説明図、第6図は同実施例の動作を説明するために示すフローチャート、第7図は同実施例のシフトレジスタ系列発生器および符号変換手段の具体例を示すブロック図、第8図は同実施例の符号変換手段の例を示すブロック図、第9図（1）～（3）は同シフトレジスタ系列の発生例と符号変換例を示す説明図、第10図は同符号変換手段の他の具体例を示すブロック図、第11図は同符号変換手段のさらに他の具体例を示すブロック図、第12図（1），（2）は同シフトレジスタ系列の発生例と符号変換例を示す説明図、第13図は他のシフトレジスタ系列の発生例と符号変換例を示す説明図、第14図はランダム符号発生R(t)の発生例を示す説明図、第15図はの変換例を示す説明図、第16図はデータパケットの基本的構成例を説明するための図、第17図は従来例のブロック図、第18図は同従来例の動作を説明するためのフローチャートである。

1…送信装置、2…伝送路、

3(0)～3(Nc−1)…受信装置、

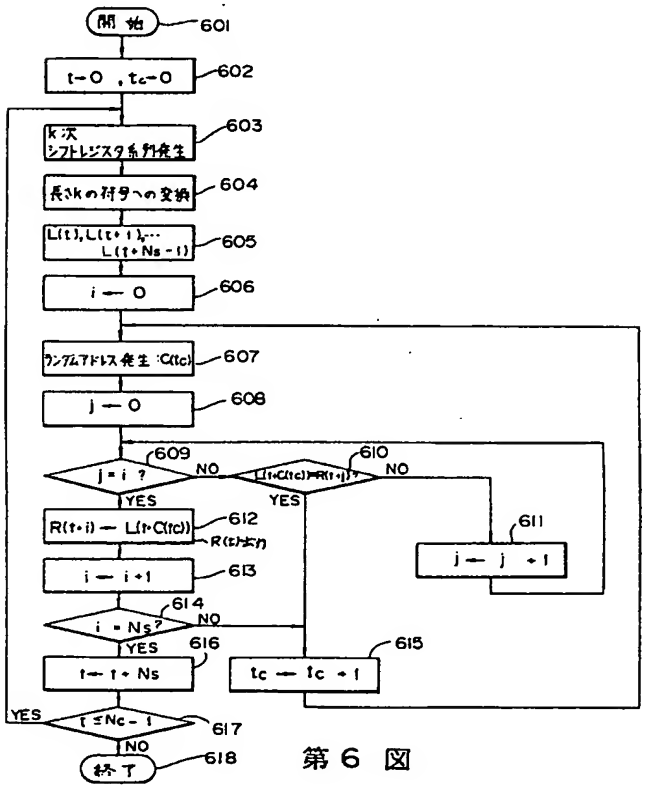
12…暗号化回路、

13…ランダム符号発生装置、

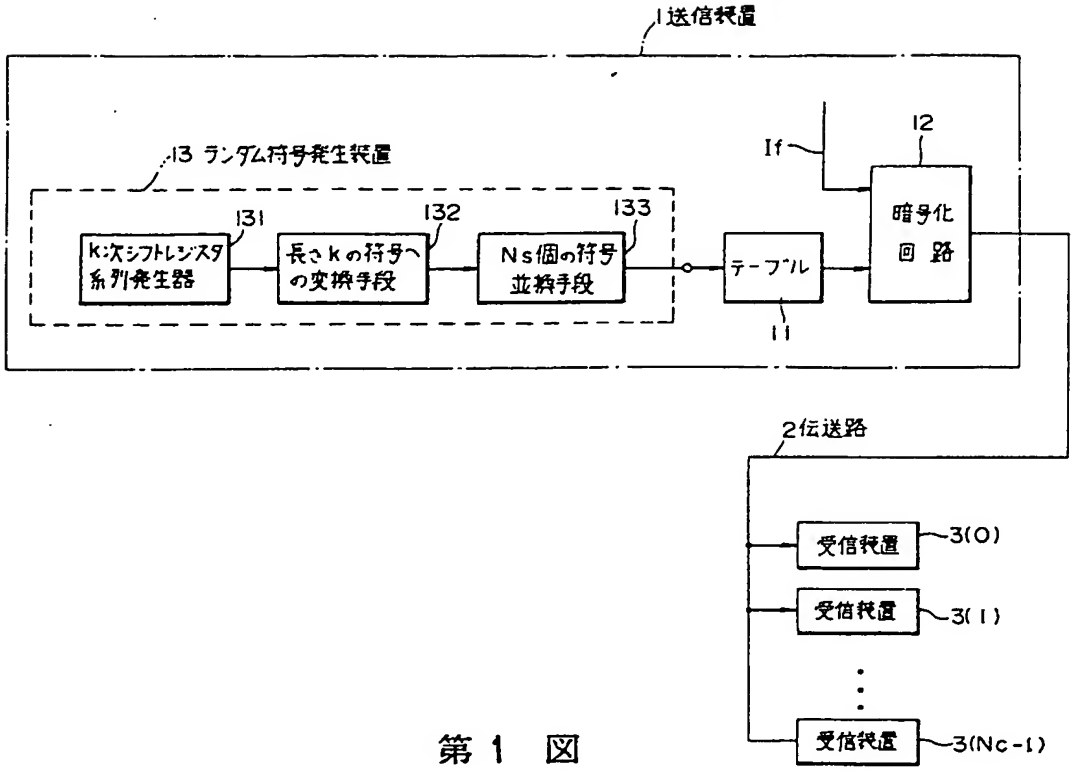
131…シフトレジスタ系列発生器、

132…符号変換手段、133…符号並換手段。

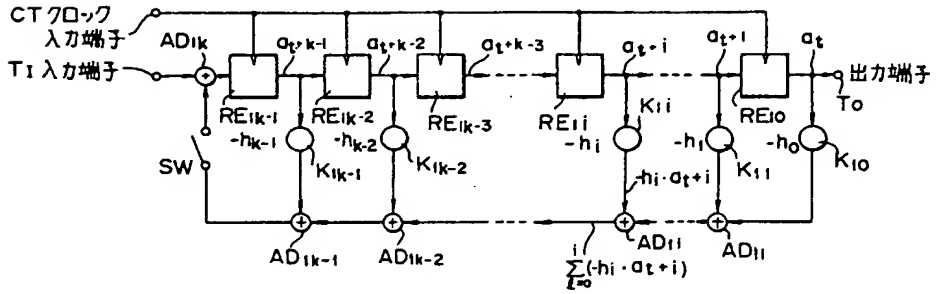
代理人　弁理士　伊藤進



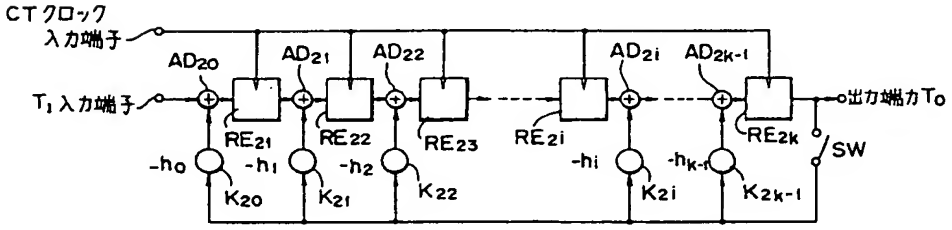
第6図


1送信装置
13 ランダム符号発生装置
131
132
133
k次シフトレジスタ系列発生器
長さkの符号への変換手段
Ns個の符号並べ手段
テーブル
11
If
12
暗号化回路
2伝送路
受信装置
3(0)
受信装置
3(1)
受信装置
3(Nc-1)

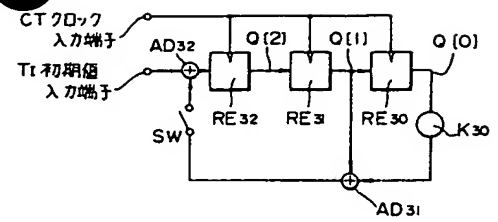
第 1 図


CTクロック入力端子
T1入力端子
ADik
SW
REik-1
REik-2
REik-3
REii
REio
出力端子
To
ADik-1
ADik-2
ADii
ADio

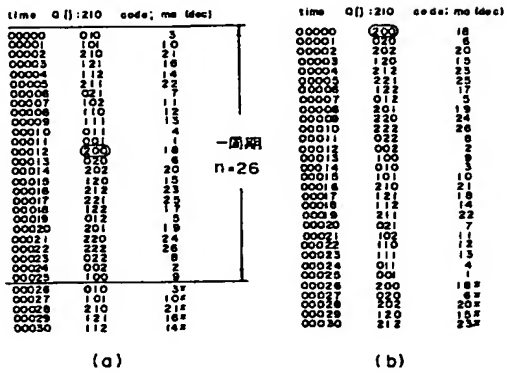
第 2 図


CTクロック入力端子
T1入力端子
AD20
AD21
AD22
AD2i
AD2k-1
RE21
RE22
RE23
RE2i
RE2k
出力端子To
SW
K20
K21
K22
K2i
K2k-1

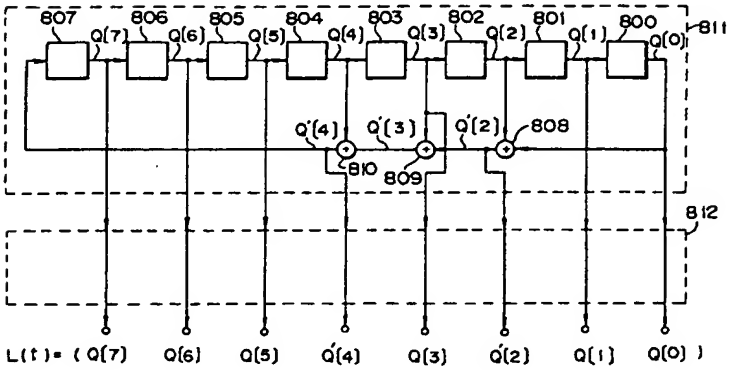
第 3 図



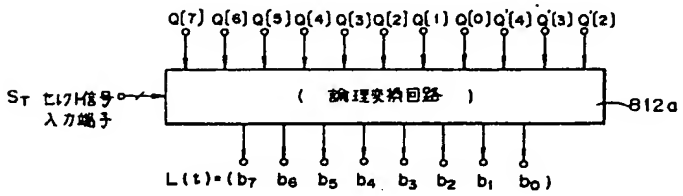
第 4 図



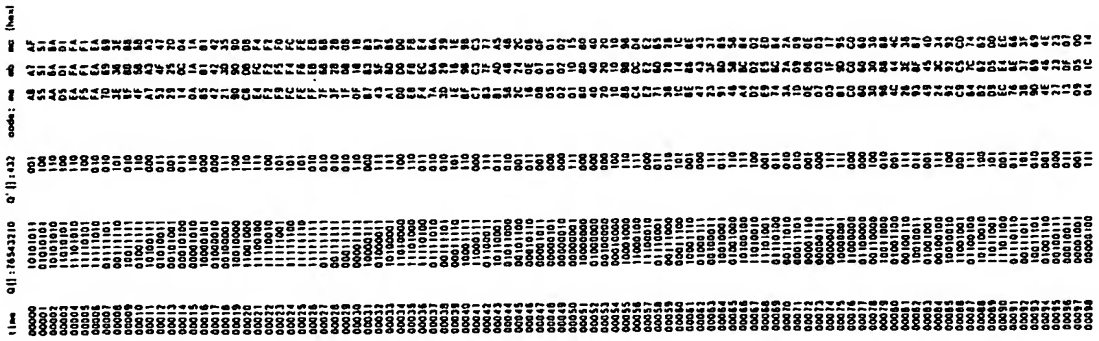
第 5 図



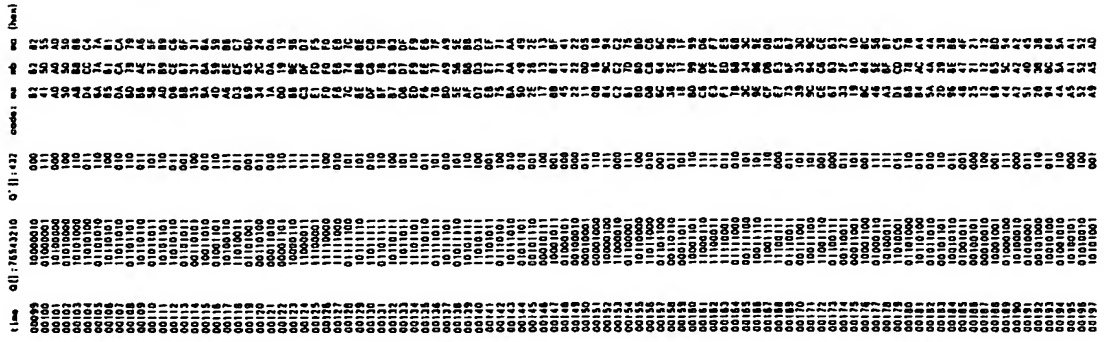
第 7 図



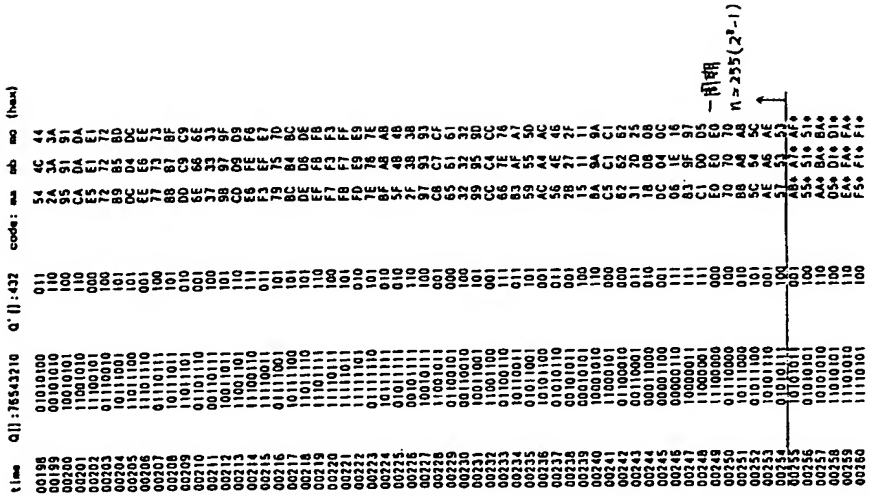
第 8 図



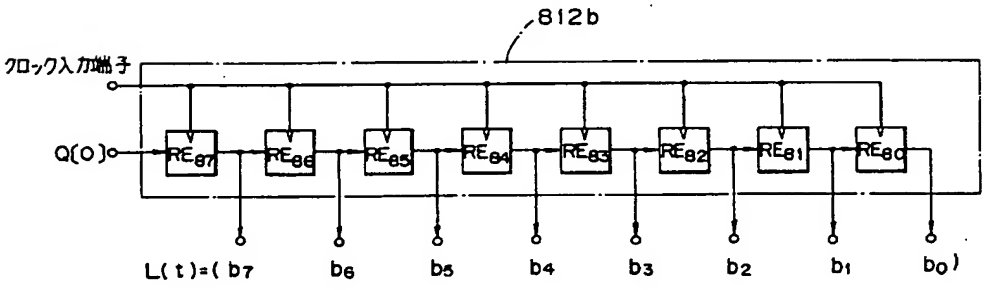
第9図 (1)



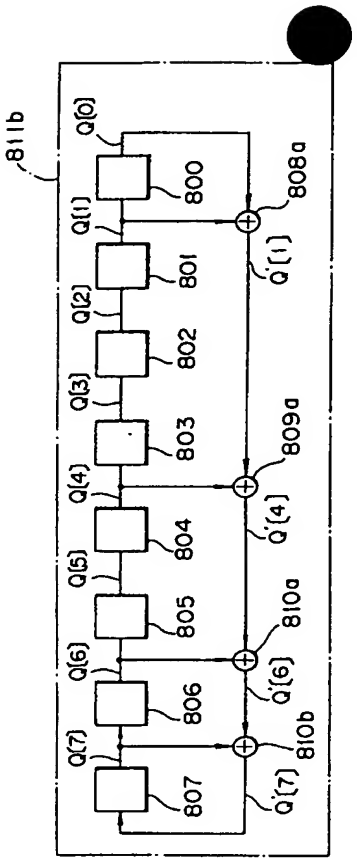
第9図 (2)


time
Q(1):76543210
Q'(1):432
code: aa
ab
ac (hex)
一周期
n = 255(2⁸-1)

第9図(3)


812b
クロック入力端子
Q(0)
RE87
RE86
RE85
RE84
RE83
RE82
RE81
RE80
L(t)=(b7 b6 b5 b4 b3 b2 b1 b0)

第10図

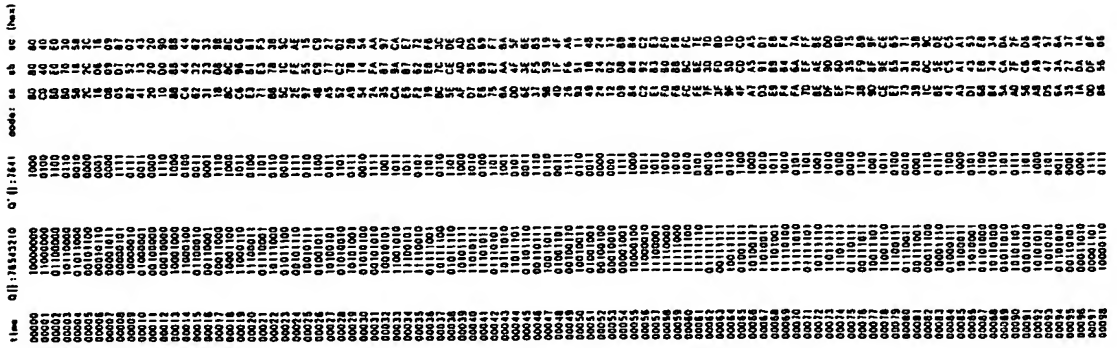


第11図

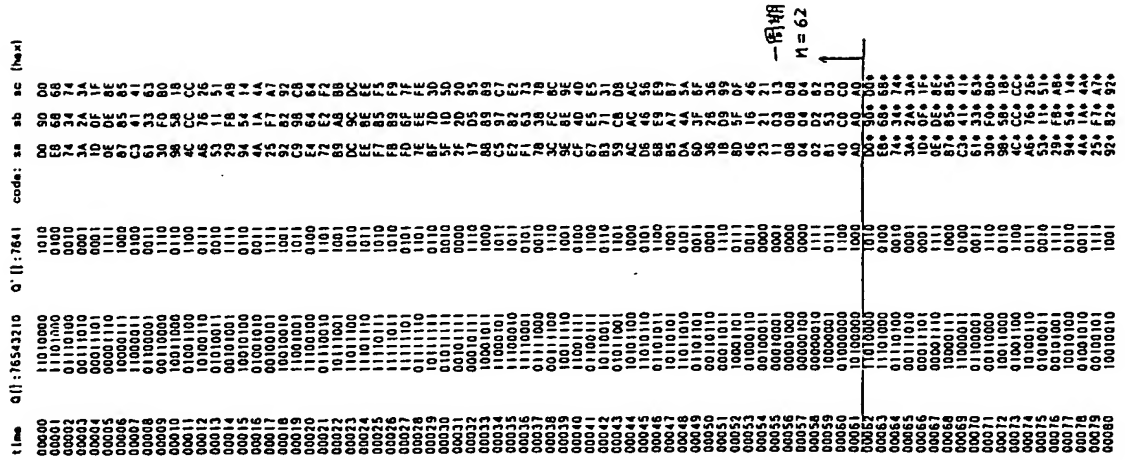
time	Q[]:76543210	Q'[]:7641	code:	sa	sb	sc (hex)
00099	01000011	1100		43	C1	C1
00100	10100001	0111		A1	73	23
00101	01010000	0010		50	10	50
00102	00101000	0000		28	28	28
00103	00010100	1110		14	D4	94
00104	10001010	0111		8A	5A	0A
00105	01000101	0011		45	17	47
00106	00100010	1111		22	F2	A2
00107	10010001	1001		91	B3	93
00108	11001000	0100		C8	48	48
00109	01100100	1100		64	E4	E4
00110	10110010	1001		B2	A2	B2
00111	11011001	0101		D9	48	58
00112	01101100	1100		6C	EC	EC
00113	10110110	1001		B6	A6	B6
00114	11011011	1010		D8	99	D9
00115	11101101	1011		ED	BF	EF
00116	11110110	0101		F6	66	76
00117	01111011	0010		7B	39	79
00118	00111101	0001		3D	2F	3F
00119	00011110	0001		1E	0E	1E
00120	00001111	0000		0F	0D	0D
00121	00000111	0000		07	05	05
00122	00000011	0000		03	01	01
00123	00000001	1111		01	D3	83
00124	10000000	1000		80*	80*	80*
00125	11000000	0100		C0*	40*	40*
00126	01100000	1100		60*	E0*	E0*
00127	10110000	0110		B0*	70*	30*
00128	01011000	0010		58*	18*	58*
00129	00101100	0000		2C*	2C*	2C*
00130	00010110	0001		16*	05*	16*

一周期
n = 124

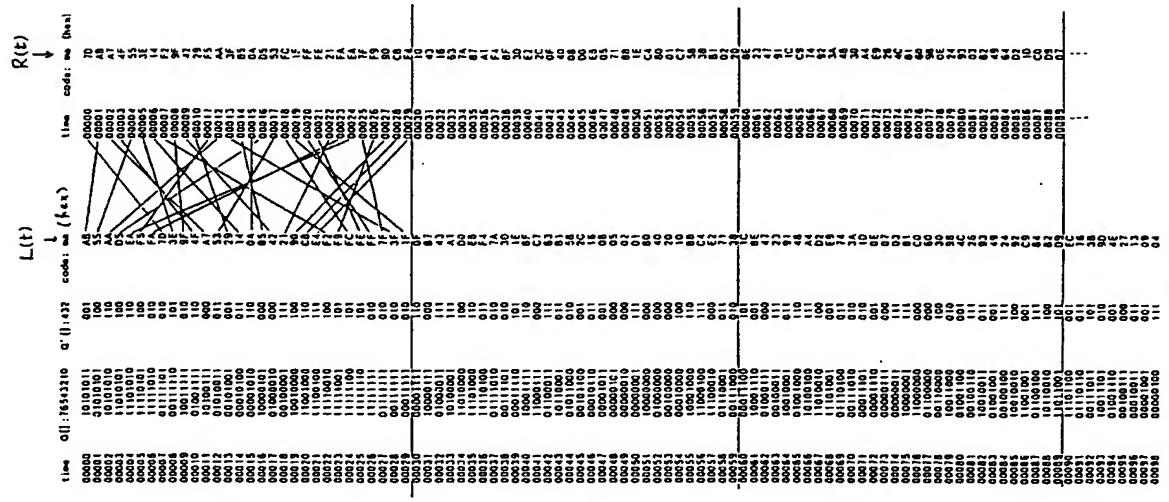
第12図 (2)



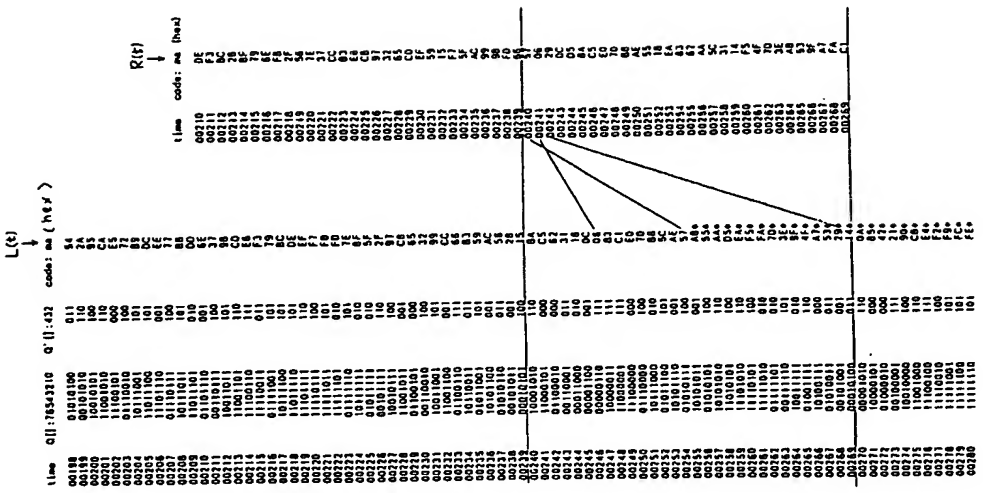
第12図 (1)



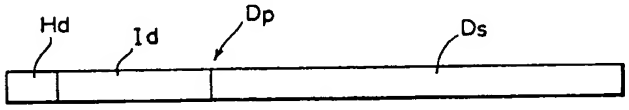
第13図



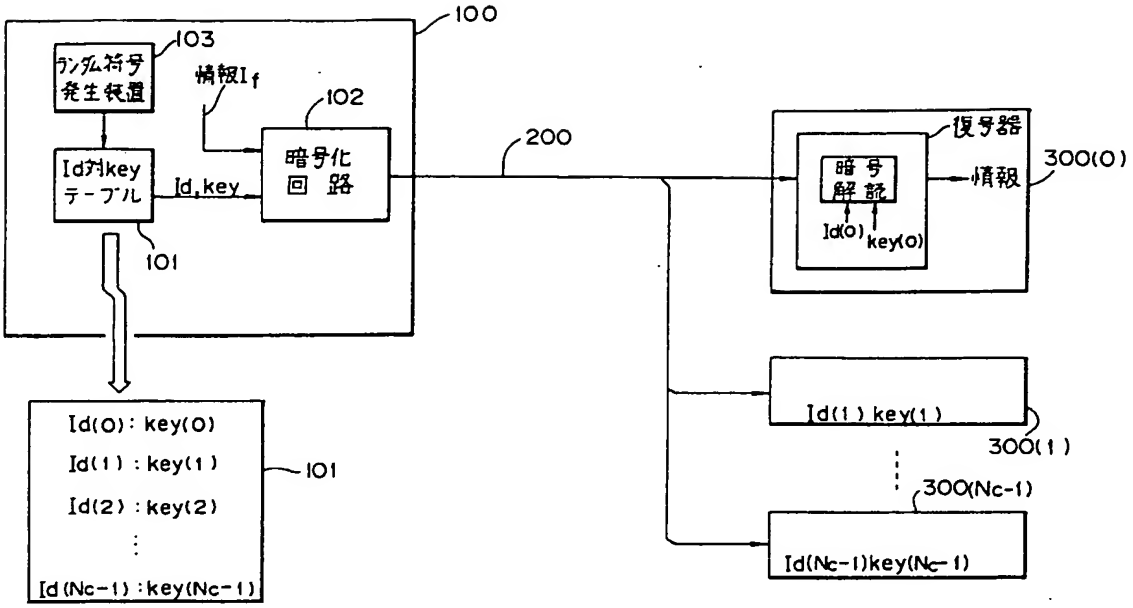
第14図



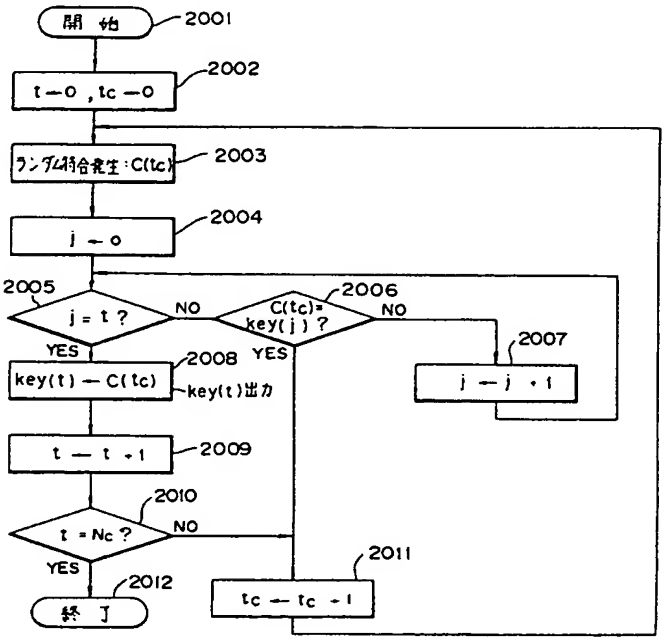
第15図



第16図



第17図



第18図